INTEGRATION DATASHEET

SpyCloud

Microsoft Defender for Endpoint

ENTERPRISE PROTECTION FOR MICROSOFT DEFENDER FOR ENDPOINT

DETECT AND REMEDIATE MALWARE INFECTIONS TO PREVENT IDENTITY-BASED THREATS

THE PROBLEM

Malware-infected devices are a launchpad for identity-based threats – feeding account takeover, ransomware, and online fraud. Even with antivirus and endpoint security solutions in place, gaps in detecting and responding to infostealer malware persist. **SpyCloud Labs discovered that 66% of infostealer-infected devices had endpoint protection installed at the time of compromise.** That means malware often slips through, and stolen identity data can remain unnoticed and in the hands of criminals.

INTEGRATION OVERVIEW

SpyCloud's integration with Microsoft Defender for Endpoint delivers definitive alerts of compromised devices that bypass existing endpoint security solutions. By continuously detecting newly recaptured identity records stolen by infostealer malware, SpyCloud provides the depth needed for complete post-infection malware remediation.

With SpyCloud's powerful identity data, your SOC team has the flexibility to define responses based on your organization's policies – from alerting to automatically isolating devices – to contain identity threats and prevent ransomware attacks.

BENEFITS AT A GLANCE

Accelerate Response
Reduce MTTD and MTTR by acting on malware-infected devices early in the attack lifecycle to prevent criminals from profiting off stolen identity data

Enhance Detection
Detect infostealer malware that bypasses EDR – including compromised identities from infections on unmanaged devices outside of corporate controls

Prevent Lateral Movement
Automatically isolate compromised endpoints to limit criminal activity and block ransomware entry points

SpyCloud

KEY CAPABILITIES

DAILY REPORTS

See lists of compromised endpoints and recaptured identity data – including hostnames, usernames, IP addresses, infection timestamps, and more

FLEXIBLE ALERTING

Route alerts to Slack, Jira, or email to fit seamlessly into your tracking and alerting workflows

CUSTOMIZABLE CONTAINMENT

Automate device isolation or initiate manual review before quarantine - your response, your rules

SIMPLE SETUP

Configure the integration with ease using SpyCloud's user interface and Defender-compatible setup options

CUSTOM TIME RANGE

Search the last 24 hours for exposed identity data or adjust your preferred timeframe directly within the integration

LIVE SCRIPT EXECUTION

Remotely trigger scripts on Defender-managed devices to accelerate incident response

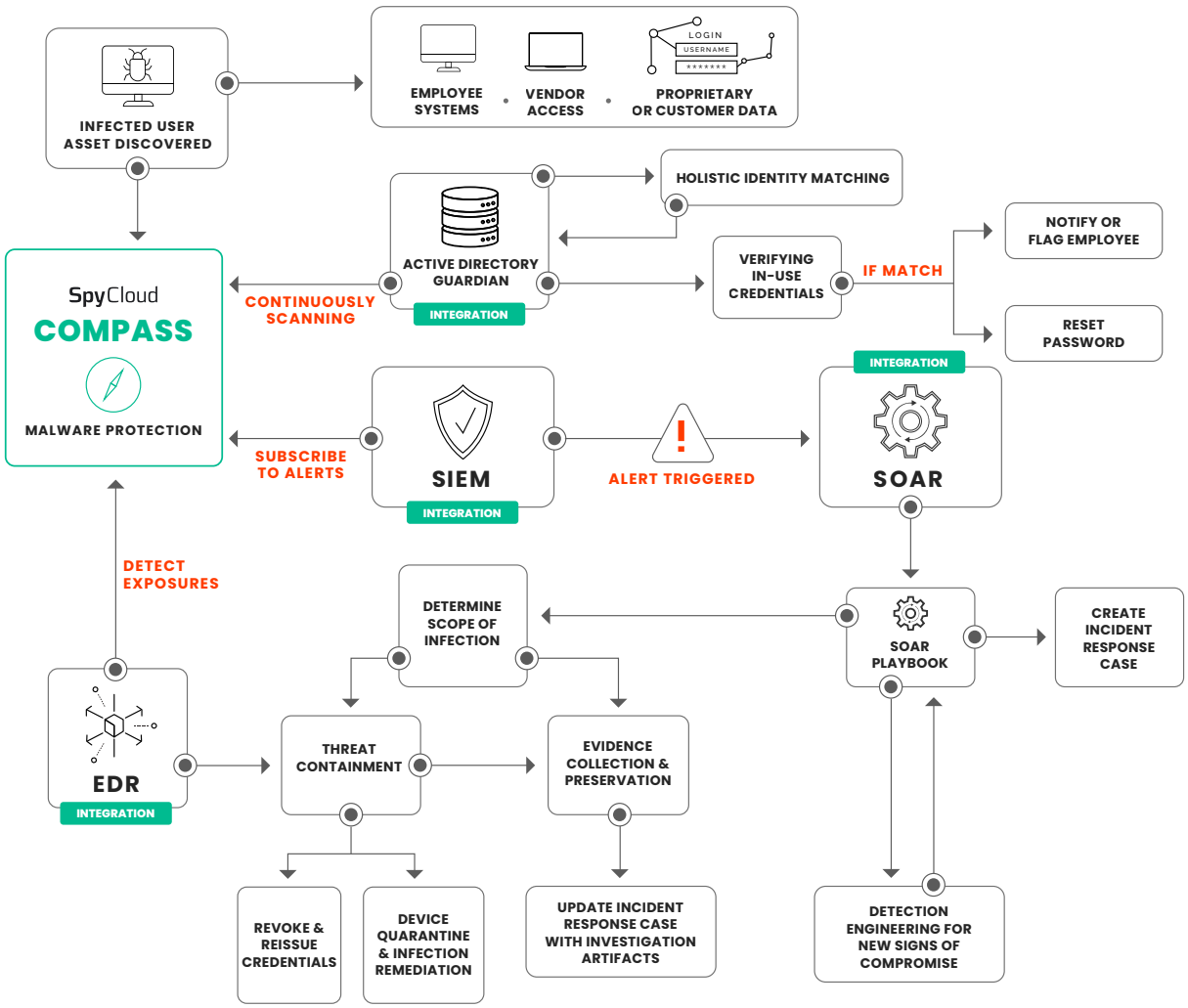
TECHNICAL REQUIREMENTS

- Microsoft Defender for Endpoint P2 License
- API Permission: The following Microsoft Defender for Endpoint API permissions must be granted
  - Machine.Read.All – Enables read access to device information
  - Machine.Isolate – Allows remote isolation of endpoints
  - Machine.LiveResponse – Enables live response session actions
  - Machine.LiveResponse.Read – Grants access to live response session results
- Feature Configuration: The following features must be enabled within Microsoft Defender for Endpoint to support SpyCloud's integration:
  - Device Read Access
  - Device Isolation
  - Live Response Actions
  - Live Response Result Retrieval
- SpyCloud Compass License
- SpyCloud Enterprise API Key

SpyCloud

SPYCLOUD INTEGRATION WORKFLOW

Example Malware Detection & Remediation Workflows:



ABOUT SPYCLOUD

SpyCloud transforms recaptured darknet data to disrupt cybercrime. Its automated identity threat protection solutions leverage advanced analytics to proactively prevent ransomware and account takeover, safeguard employee and consumer accounts, and accelerate cybercrime investigations. SpyCloud's data from breaches, malware-infected devices, and successful phishes also powers many popular dark web monitoring and identity theft protection offerings. Customers include seven of the Fortune 10, along with hundreds of global enterprises, mid-sized companies, and government agencies worldwide. Headquartered in Austin, TX, SpyCloud is home to more than 200 cybersecurity experts whose mission is to protect businesses and consumers from the stolen identity data criminals are using to target them now.

To learn more and see insights on your company's exposed data, visit **spycloud.com**